IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

UNITED STATES OF AMERICA	)	
	)	
v.	)	NO.: 3:08-cr-142
	)	JUDGES PHILLIPS/SHIRLEY
DAVID C. KERNELL	)	

SECOND MOTION TO SUPPRESS EVIDENCE OBTAINED AS RESULT OF GOVERNMENT'S UNAUTHORIZED ACCESS OF THE LAPTOP COMPUTER

Comes the defendant, David C. Kernell, through undersigned counsel and pursuant to Rules 12 and 41 of the Federal Rules of Criminal Procedure and the Fourth Amendment to the U.S. Constitution, and hereby respectfully moves this Court for an Order suppressing any information or documents obtained from the forensic searches of the computer seized from Mr. Kernell's apartment in September 2008.

I. INTRODUCTION

In his initial Motion to Suppress, Mr. Kernell showed that the search warrant to seize the laptop computer did not allow the government to examine the entirety of the computer's contents, unless it was a general warrant in violation of the Fourth Amendment, and therefore the government should have obtained a separate search warrant with limiting search protocol after the computer was seized. See [Doc. 20 at 16] (cautioning that a constitutional search warrant cannot authorize "searches of infinite duration and unlimited scope").

On July 16, 2009, this Court heard argument on two of Mr. Kernell's motions, including the motion to suppress. See [Doc. 66].[1] After both parties' arguments on the motion to suppress had concluded and the Court was listening to arguments about whether to approve pretrial

[1] Mr. Kernell began his argument on the Motion to Suppress by framing his dispute with the search warrant as follows: a search warrant issued based on probable cause to seize limited files from the computer, but the computer has been examined as if there were no limitations.

subpoenas, Mr. Kernell and his counsel learned for the first time that the government sought and obtained a warrant to search the laptop computer five months earlier (in February 2009), six months after it was seized from Mr. Kernell's apartment (in September 2008).[2] At no time after Mr. Kernell filed the Motion to Suppress did the government produce or allude to the existence of a second search warrant, even though Mr. Kernell argued, beginning in January 2009, that the government should have sought a second, more particularized search warrant. [Doc. 20 at 9, 22].

The affidavit in support of the second search warrant proves that the government knew and understood that it lacked the authority to conduct a limitless examination of the seized computer. Although the government to date has successfully sought to prevent Mr. Kernell from putting on evidence showing the extent and timing of the examinations, it is clear from the information that has been provided that the government had already extensively examined the computer before asking the Court's permission in February 2009. The undisclosed affidavit admits that the government needed judicial authority for a forensic examination of the computer, and this Court appears to have agreed by issuing the warrant, which means the search conducted prior to the issuance of the second warrant was unauthorized. A forensic evaluation of the computer done outside the time limitations of the second warrant likewise was unauthorized. Furthermore, the newly disclosed affidavit contains an explicit admission that it is possible to restrict a forensic evaluation to certain relevant matters in exactly the way Mr. Kernell has shown the government should have restricted its examination to the particular items listed in the first paragraph of the original warrant. The government could have restricted its search to items for which the Court found probable cause, but it chose not to do so.

[2] On July 16, 2008, this Court ordered that "[t]he Government shall produce a copy of the Affidavit and 2nd Search Warrant within 24 hours plus any other discovery not produced." [Doc. 66]. In court, the government provided a copy of the search warrant and affidavit. After a request from Mr. Kernell's counsel, the government produced the incorporated attachments (approx. 350 pages) to the search warrant affidavit and the return today, July 27, 2009.

II. FACTUAL BASIS FOR THIS MOTION

The events that are relevant to this Motion took place between September 2008 and July 2009, and the timing of these events is revealing: at least four months after the government seized and began forensically searching the computer, the government applied to this Court for a warrant to search the computer but did not describe the extent to which that the computer had already been searched;[3] one month after Mr. Kernell moved to suppress any unconstitutionally acquired computer evidence and argued that the government should have sought a second warrant to search the seized computer, the government sought a second search warrant;[4] six months after Mr. Kernell moved to suppress any unconstitutionally acquired computer evidence and argued that the government should have sought a second search warrant, the existence of the second search warrant was revealed for the first time; two weeks after the government claimed that "[t]he process of searching through a computer . . . necessarily requires agents to inspect some items that are not called for by the warrant,"[5] a federal law enforcement agent submitted an

[3] Mr. Kernell cannot state the facts with precision without an evidentiary hearing. On or about October 17, 2008, the government informed Mr. Kernell's counsel about what had thus far been found on the computer. When Special Agent Scott A. Wenger applied for a search warrant to search the computer seized five months earlier, see (*Application and Affidavit for Search Warrant*, In the matter of the Search of Acer Aspire 3000 Laptop Computer Previously Taken From Apartment, 3:09-MJ-1028 02/26/2009) (hereinafter "02/26/09 *Affidavit*), he explained that the government was "applying for an additional warrant to search the SUBJECT COMPUTER and seize evidence described in Attachment B." Id. ¶ 3. The Affidavit described the first search warrant as authorizing the computer's "seizure." Id. ¶ 5.

[3] Mr. Kernell argued that a second search warrant was required beginning on January 9, 2009. [Doc. 19 at 9, 22]. The existence of the second search warrant was revealed July 16, 2009. See [Doc. 66].

[4] On January 9, 2009, Mr. Kernell filed a Motion to Suppress in which he argued that the government should have sought a second, more particularized search warrant. [Doc. 20 at 9, 22]. On February 26, 2009, Special Agent Scott A. Wenger applied for a search warrant to search the computer seized five months earlier. (02/26/09 *Affidavit*).

[5] Mr. Kernell had argued that a limiting protocol should have been employed to limit the scope of a search to documents for which there was probable cause. [Doc. 20]. The government responded on February 13, 2009, to the Motion to Suppress and took the position that the search warrant not only authorized agents to seize the computer but that it "also authorize[d] agents to search through that seized computer for those records [called for by the warrant]" and that "[b]ecause the warrant authorized the agents to search for particular computer records, it therefore authorized them to look through the Defendant's computer for those records." [Doc. 22 at 1, 6].

affidavit that admitted that "[i]n some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence;"[6] one week after Mr. Kernell renewed his argument that a second search warrant was required to comply with the Fourth Amendment, the government sought a second search warrant;[7] one week before the scheduled evidentiary hearing on the Motion to Suppress, the government claimed for the first time that Mr. Kernell was not entitled to an evidentiary hearing and tried to argue that the only issue was whether "the" warrant granted authority for "an 'examination of all files on' defendant's computer";[8] one day before the scheduled evidentiary hearing, the government filed a motion to quash the two subpoenas served on federal agents for their testimony about the execution of the search warrant and scope of any forensic examinations of the computer;[9] and at no time during the hearing on Mr. Kernell's motion to suppress did the government mention the existence of a second search warrant, though Mr. Kernell's counsel argued that the government should have obtained a second, particularized search warrant to make the search comply with the Fourth Amendment to the U.S. Constitution.

A. <u>Search Warrant for Apartment ("First Search Warrant")</u>.

On September 20, 2008, Special Agent Andrew M. Fisher of the F.B.I. submitted an application and affidavit for a warrant to search Mr. Kernell's apartment. (*Application and*

[6] On February 13, 2009, the government filed its response in opposition to Mr. Kernell's Motion to Suppress [Doc.22 at 7], and on February 26, 2009, the government sought a second search warrant that admitted that limiting protocols exist which could be used.

[7] On February 20, 2009, Mr. Kernell replied to the government's response in opposition to his motion, and again questioned whether the search warrant comported with the Fourth Amendment requirements or whether a second search warrant should have issued. [Doc. 27 at 19].

[8] [Doc. 61 at 3, 2] ("The dispute is not over *whether* agents examined things on the hard drive in order to determine whether they were among those things authorized to be seized, but whether the warrant granted the Untied States that authority as a matter of law."); ("[W]hether there was an 'examination of all files on' defendant's computer is not disputed.").

[9] [Doc. 64].

Affidavit for Search Warrant, including attachments, In the matter of the Search of Room A, 3:08-MJ-1084, 9/20/2008) (hereinafter "09/20/08 *Affidavit*"). The Affidavit contained two attachments. Id.

> This affidavit is submitted in support of the issuance of a warrant authorizing the **search** of the premises described in Attachment A. The purpose of the search is the location and **seizure** of items described in Attachment B.

(9/20/08 *Affidavit* ¶ 6) (emphasis added). Attachment A consisted of photographs, a drawing, and a description of an apartment; Attachment B listed the computer and certain documents and computer files. Id.

Agent Fisher's application to this Court sought permission to seize a computer and a list of "documents and computer files" set out in the first paragraph of Attachment B to the Affidavit (hereinafter referred to as "Paragraph 1"). The Affidavit discussed searching computer systems for computer evidence, but it did so in order to justify seizing the entire computer rather than performing an on-site search. The Affidavit neither outlined a forensic search protocol nor directly stated that a search would be conducted pursuant to the instant warrant. See (9/20/08 *Affidavit* ¶ 33) (concluding that "it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized"); id. ¶ 32(b) ("[s]earching computer systems . . . . often require[s] the seizure of most or all of a computer systems input/output peripheral devices, related software, documentation, and data security devices . . ."); id. ¶ 33 ("seized and subsequently processed"); see also id. at ¶ 32.[10]

The Warrant commanded agents to "search" on or before September 29, 2008. (9/20/08 *Search Warrant & Return*). The Return indicates that the warrant was executed 11:55 p.m. on

[10] The Affidavit refers to searching, but when the affiant describes what he seeks authorization to do, the term "search" precedes "seizure," so the use of the term is not dispositive of the issue before this Court. See (9/20/08 *Affidavit* at p. 11); id. ¶ 30 ("Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware . . . .").

September 20, 2008 and that a laptop computer was "taken pursuant to the warrant." Id.

In his Motion to Suppress filed in January 2009, Mr. Kernell questioned whether a single warrant could sufficiently grant authority to search an apartment, seize a computer, and subsequently search the seized computer:

> Because there are at least two stages to the computer search process, including the physical search for the computer hardware and the later electronic search to retrieve specific data, the warrant did not sufficiently limit the discretion of a forensic analyst during a subsequent search. The purpose of seizing a computer, after all is to further search it. The small physical size of a computer belies the amount of information contained within it. There are no sufficiently valid portions of the attachment which can be severed from the overbroad.

[Doc. 20 at 15-16]. The government agreed in writing that there are two stages when a computer is seized, [Doc. 22 at 2], and further acknowledged that a forensic examination constitutes a subsequent search when it sought a second warrant to search the computer.

B. **Search Warrant for Computer ("Second Search Warrant")**.

When Special Agent Scott A. Wenger applied for a warrant in February 2009 to search the computer seized in September 2008, see (*Application and Affidavit for Search Warrant*, In the matter of the Search of Acer Aspire 3000 Laptop Computer Previously Taken From Apartment, 3:09-MJ-1028 02/26/2009) (hereinafter "02/26/09 *Affidavit*"), he explained that the government was "applying for an additional warrant to search the SUBJECT COMPUTER and seize evidence described in Attachment B." Id. ¶ 3. As in the first search warrant, Attachment A described the property to be searched while Attachment B described the property concealed thereon (i.e., "items to be seized"). (02/26/09 *Search Warrant*). The Warrant commanded Agent Wenger to search on or before March 7, 2009." Id.

The Affidavit described the first search warrant as authorizing the computer's **seizure**. Id. ¶ 5. The second search warrant was sought, explained the affiant, to find "evidence of

violations of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B), and (e)(2), Section 1028(d)(7), Section 1343, Section 879, Section 875(c), and Section 1519." (02/26/09 *Affidavit*). A Superseding Indictment had been returned three weeks earlier for four of six of those crimes. [Doc. 21]. The Affidavit informed as follows:

> 18. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT COMPUTER, in whatever form they are found. I submit that there is probable cause to believe those records are stored in the SUBJECT COMPUTER . . . .
>
> 19. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designated to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

(02/26/09 *Affidavit* at ¶¶ 18-19).

C. **Non-Evidentiary Suppression Hearing**.

In order to avoid an evidentiary hearing, the government first filed a motion opposing the long-requested evidentiary hearing because "[b]ased on the defendant's motion, and filings before the Court, the United States understands that the hearing will address the sufficiency of the affidavit in support of the warrant, only," [Doc. 61 at 5], then subsequently filed a motion to quash, arguing that "it is not clear why [the search warrant affiant] has been subpoenaed, since the Defendant apparently does not intend to ask him about the facts presented in his affidavit." [Doc. 64 at 2].

At the hearing on the motion to suppress, Mr. Kernell emphasized that an evidentiary hearing was necessary because the manner of the execution of the search warrant was unconstitutional. See also [Doc. 65 at 3] ("The agents will be asked to explain how, when, where, for how long, and to what extent the computer was searched."). This is a separate issue from the facial or legal validity of a warrant, because "a seizure that is lawful at its inception can violate the Fourth Amendment if its manner of execution unreasonably infringes interests protected by the Constitution." Illinois v. Caballes, 543 U.S. 405 (2005) (citing United States v. Jacobsen, 466 U.S. 109 (1984); see also United States v. King, 227 F.3d 732, 751 (6th Cir. 2000) (noting that "a valid search warrant can turn into an invalid general search if officers flagrantly disregard the limitations of the warrant" and providing that the "test for making such a determination is whether the officer's actions were reasonable") (search of basement pursuant to valid warrant to search downstairs unit of dwelling unreasonable and suppressing cocaine recovered as result of illegal search); United States v. Corrado, 803 F.2d 1280 (M. D. Tenn. 1992) (suppressing evidence and holding that "the officers exceeded the scope of the search warrant by remaining in the house for more time than was reasonably necessary to execute the search warrant"). The disregard for the limitations of the original warrant also goes beyond just a question of whether the government examined each file. There are questions of how it was done, what keywords or other search methods and forensic programs were used, the time, extent, and whether any attempts were made to restrict the search results to the particularized files.

In Illinois v. Caballes, 543 U.S. 405 (2005), the Supreme Court held that the use of a narcotics dog was not an unconstitutional search because it only revealed unlawful information (i.e., the existence of a contraband substance) and found the holding consistent with Kyllo v. United States, 533 U.S. 27 (2001), the case in which the Supreme Court underscored that it is

courts' role to ensure privacy despite technological change and held that the use of a thermal-imaging device constituted an unlawful search. According to the Caballes Court, "[c]ritical to [Kyllo] was the fact that the device was capable of detecting lawful activity . . . ." Id. Computers are vast repositories of personal information in which individuals have a recognized privacy interest. See Guest v. Leis, 255 F.3d 324 (6th Cir. 2001); United States v. Mitchell, 565 F.3d 1347 (11th Cir. 2009) ("Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives."). A forensic search of a computer full of lawful content is unlike the dog-sniff in Caballes such that the manner in which a forensic search of a computer is conducted and the extent to which it exposes lawful conduct is a relevant inquiry for an evidentiary hearing.

In addition, Mr. Kernell requested an evidentiary hearing because the manner of execution is directly tied to the scope of authority granted under a warrant, because probable cause to seize some files does not provide probable cause to examine the entire computer, and because the government cannot rely on an electronic device or forensic program to circumvent the probable cause requirement of the Fourth Amendment. See Ybarra v. Illinois, 444 U.S. 85 (1979) ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."). Cf. People v. Prinzing, 907 N.E.2d 87 (Ill. Ct. App. 2009)[11] (reversing defendant's conviction for possession

[11] According to Detective Smith, he initially used a noninvasive tool to perform a "preview," which prevents any changes from happening to the computer when the system is turned off and on. The "preview" allows detectives to view the hard drive but prevents them from making any changes to any of its files. Normally, after the "preview" program, Detective Smith would use a program called "Image scan." The image scan looks for images related to Web pages to get a history of pages that the user has visited. The program brings up thumbnail images from Web pages. Depending upon what is found, he then would use a tool that would look for viruses or any key stroke loggers, which capture key strokes and send the information to a remote location.

of child pornography because officer's search exceeded scope of consent) (evidentiary hearing held); United States v. Richardson, 583 F.Supp.2d 694, 716 (W.D. Pa. 2008) (police obtained consent to search the defendant's computer then used a forensic image scanning disk to search the computer's hard drive for images, which the court determined exceeded the scope of the defendant's original consent to search for evidence of credit card fraud on the Internet). An evidentiary hearing is even more necessary now that it has been revealed that the government sought a second warrant to search the computer after it had already conducted an examination.

III. THE GOVERNMENT'S SEARCHES OF THE COMPUTER WERE NOT AUTHORIZED IN THE FALL OF 2008, AND THE GOVERNMENT CANNOT NOW TAKE A POSITION INCONSISTENT WITH ITS APPLICATION FOR A WARRANT TO SEARCH THE COMPUTER IN FEBRUARY 2009.

The first search warrant authorized the government to seize a computer it had probable cause to believe contained the records listed in Paragraph 1 of Attachment A; but a second warrant was required to search the computer for those records. Although this is not a new argument, the existence of the second search warrant proves it conclusively. As set forth in Mr. Kernell's first Motion to Suppress:

> (1) The warrant authorized the seizure of a laptop computer and a limited number of files;[12]
> (2) Once seized, the government exceeded the scope of its authority by examining all of the computer's contents without the judicial approval to do so.
> (3) At minimum, the government could and should have submitted a search protocol for judicial approval that would have limited all subsequent searches to those files for which there was probable cause.
> (4) The only way the warrant could be read to authorize such electronic rummaging through documents and files would transform it into a general warrant.
> (5) General warrants are prohibited by the Fourth Amendment to the U.S. Constitution.

People v. Prinzing, 907 N.E.2d 87, 91 (Ill. Ct. App. 2009).

[12] [Doc. 20 at 1].

(6) If, as the affidavit states, it was not feasible to seek judicial approval of a search protocol before seizing the computer, the Constitution required the government to limit the search after the seizure by seeking judicial approval.

[Doc. 20 at 1-2]. Therefore, if all subsequent forensic examinations of the computer have been pursuant to the first search warrant, as claimed by the government, the government has searched without authority. What the government denies in its pleadings (i.e., that a particularized warrant was required to search the computer and that a limited search was infeasible), it has admitted, both by actions taken and sworn statements included in an affidavit submitted to this Court. The government may wish to rely only on the first warrant, but it cannot deny the existence or significance of the second warrant.

A. The Undisclosed Affidavit Admits that the Government Lacked Authority to Perform "Extensive" Searching.

When the government made sworn application to a U.S. Magistrate Judge for authority to search the laptop computer in February 2009, the Affidavit indicated that "carefully targeted searches" are "possible" but that "more extensive searches, such as scanning areas of the disk not allocated to listed files, or perus[ing] every file" was the proper course in this case. (02/26/09 *Affidavit* ¶ 19). In fact, the available evidence indicates "extensive" searching had already been conducted, and the government's application for a second search warrant admits that the government previously lacked authority to search the computer at all, let alone search the computer in a non-targeted manner.

1. When the Government Sought a Warrant to Search the Computer, the Government Admitted that It Previously Lacked Authority to Search.

When applying for the second search warrant, the government made two admissions. See Black's Law Dictionary (8th ed. 2004) ("admission"); Fed. R. Evid. 801(d)(2). First, the act of seeking a second warrant was itself an admission by the government that it lacked authority

under the original warrant to search the computer. Some cases hold that when there has been an illegal search, a second search warrant can validly issue if it is issued based on independent probable cause and knowledge gained during the prior illegal search is not used to obtain the second warrant. See Murray v. United States, 487 U.S. 533 (1988); Segura v. United States, 468 U.S. 796 (1984). Implicit in the request for a second search warrant, therefore, is that the first search was illegal or that the first search warrant was invalid or insufficient to convey the requested authority. Unlike the cases in which second search warrants issue, though, the government has indicated that it will not rely on the second warrant, even though it was provided to some of the forensic examiners.

Second, the affidavit in support of the warrant included the admission that "carefully targeted searches" can be conducted on computers. As sworn in the second search warrant affidavit:

> In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring time-consuming manual search through unrelated materials that may be commingled with criminal evidence.

(02/26/09 *Affidavit*). Therefore, when the government swore to this Court and argued in its pleadings that it is "required to examine all data"[13] and "necessarily require[d] . . . to look at irrelevant files,"[14] the government was really making a choice to reject the technological or judicial mechanisms that are available to limit a computer search.

---

[13] See (09/20/08 *Affidavit*) ("Searching authorities are required to examine all data to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity.").

[14] [W]hether there was an "examination of all files on" defendant's computer is not disputed. In its opposition, the United States agreed that its agents would "look through the defendant's computer for" the computer records particularly described in the warrant, and argued that search "**necessarily requires agents to look at irrelevant files**." Whatever minor disputes might remain – such as whether agents personally "examined" everything, as opposed to relying upon software to search for keywords – are not material to the issues before the Court.
07/09/09 *Response to Defendant's Motion for Separate Evidentiary Hearing* [Doc. 61 at 2] (emphasis added).

In its response to Mr. Kernell's motion, the government informed that, "As with any search, 'the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.'" [Doc. 22 at 10]. On the eve of the hearing on the motion to suppress, though, the government argued that an evidentiary hearing was unnecessary (1) because the motion rested "upon only undisputed factual questions," [Doc. 61 at 3] though Mr. Kernell still has no facts about "how, when, where, for how long, and to what extent the computer was searched," [Doc. 65 at 3], and (2) because Mr. Kernell had been given the "result" of the forensic evaluations of his computer, though the results do not reveal the "manner" of the searching. [Doc. 62 at 2]. For example, the primary CART report contains no indication as to when the searches were conducted.

In essence, when the government now argues that the first warrant authorized the government to examine all files on the computer and proposes that this Court consider that question in the abstract, the government is really saying that -- despite its demonstrated ability to make particularized requests and admitted ability to perform particularized searches -- performing "extensive" rather than "carefully targeted searches" is *per se* reasonable, even absent factual proof about the extent to which searches were performed in a particular case. However, unnecessary and unjustified extensive searching directly contravenes the purpose of the Fourth Amendment's particularity requirement.

> By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justification, and will not take on the character of the wideranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79 (1987); Marron v. United States, 275 U.S. 192 (1927) (reminding that the purpose of the Fourth Amendment's particularity requirement is to make "general searches . . . impossible and prevent[] the seizure of one thing under a warrant

describing another" such that "nothing is left to the discretion of the officer executing the warrant"). See also United States v. Abboud, 438 F.3d 554 (6th Cir. 2006) (warrant overbroad); United States v. Ford, 184 F.3d 554 (6th Cir. 1999) (warrant overbroad); United States v. Blakeney, 942 F.2d 1001 (6th Cir. 1991) (describing general warrants as authorizing "rummaging"). The reasonableness of a search is not an abstract question. It requires an evidentiary hearing.

2. *The Government is Estopped From Denying the Sworn Statements Made in the Affidavit and/or that It Did Not Have Authority to Search the Computer Prior to the Second Search Warrant in February 2009.*

On September 26, 2008, the first search warrant was returned to the magistrate judge designated on the warrant, and the Return indicated that an "Acer Aspire 3000 laptop computer" and other items had been taken pursuant to the warrant. (09/20/08 *Search Warrant Return*). Special Agent Scott Wenger is the agent who signed the Return and swore that the inventory provided "a true and detailed account" of the property taken. Id. Five months later, Agent Wenger submitted another affidavit to the same magistrate judge:

> I am a Special Agent and have reason to believe that on the property known as ACER ASPIRE 3000 LAPTOP COMPUTER previously taken from [Mr. Kernell's apartment] and currently in the custody of the FBI in Knoxville, TN, there is now **concealed** certain property, namely that property described in Attachment B to the Affidavit in Support hereof all of which is evidence of violations of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B), and (e)(2), Section 1028(d)(7), Section 1343, Section 879, Section 875(c), and Section 1519.

(02/26/09 *Application and Affidavit for Search Warrant*) (emphasis added). The Affidavit informed that:

> 3. I make this affidavit . . . for a warrant to search an Acer Aspire Laptop computer . . . which was seized pursuant to a search warrant on September 20, 2008, as further described below. Since the SUBJECT COMPUTER was seized, it has remained in the possession of the FBI located at 710 Locust Street, Knoxville, TN.

> 4. Based on evidence obtained during the continuing investigation of the unauthorized access to Alaska Governor Sarah Palin's Yahoo! E-mail accounts, I am applying for an additional search warrant to search the SUBJECT COMPUTER and seize evidence described in Attachment B. I am applying for the warrant in light of additional evidence obtained since the issuance of the warrant on September 20, 2008 and in view of the superseding Indictment in this case. . . .
>
> 18. As described above and in Attachment B, this application seeks **permission to search and seize records that <u>might</u> be found** on the SUBJECT COMPUTER, in whatever form they are found. . . .
>
> 20. Based on the foregoing, I respectfully submit that this affidavit supports probable cause for a warrant to search the SUBJECT COMTPUER and seize the items described in Attachment B.

(02/26/09 *Affidavit*) (emphasis added). A warrant issued based on the facts outlined in the Affidavit.

The government is estopped from arguing that it had authority to extensively search the computer prior to the issuance of the second search warrant in February 2009.

There is no "flat rule" absolutely prohibiting a party from invoking the doctrine of estoppel against the government. <u>See</u> <u>Michigan v. City of Allen Park</u>, 954 F.2d 1201 (6th Cir. 1992) (citing <u>Heckler v. Community Health Services</u>, 467 U.S. 51 (1984)). In fact, the doctrine of judicial estoppel has been applied against the government in criminal cases. <u>See e.g.</u>, <u>United States v. Issacs</u>, 708 F.2d 1365 (9th Cir. 1983); <u>People v. Gross</u>, 465 N.E.2d 119 (Ill. Ct. App. 1984) (state estopped from asserting that a purse not owned by defendant such that it was within scope of search warrant because the suppressing hearing record established that the officer conducting the search knew that the purse belonged to the defendant); <u>People v. Jones</u>, 217 N.W.2d 884 (Mich. Ct. App. 1974) (state estopped from asserting that witnesses were not *res gestae* witnesses and also that they were accomplices); <u>United States v. Bagley</u>, 772 F.2d 482 (9th Cir. 1985) (government not permitted on appeal to contest defendant's standing to challenge

search of car because it had argued at trial that defendant was driving the car during robbery); People v. Lawlor, 683 N.E.2d 213 (Ill. Ct. App. 1997) (state estopped from arguing that a seizure order was actually a search warrant).

Although it is generally understood that the government may not be prohibited from proceeding on alternate theories in a criminal case, see United States v. Cassiere, 4 F.3d 1006 (1st Cir. 1993), the doctrine of judicial estoppel prevents the government from taking inconsistent positions. The Supreme Court's general discussion of the doctrine is instructive:

> "[W]here a party assumes a certain position in a legal proceeding, and succeeds in maintaining that position, he may not thereafter, simply because his interests have changed, assume a contrary position, especially if it be to the prejudice of the party who has acquiesced in the position formerly taken by him." This rule, known as judicial estoppel, "generally prevents a party from prevailing in one phase of a case on an argument and then relying on a contradictory argument to prevail in another phase."
>
> Although we have not had occasion to discuss the doctrine elaborately, other courts have uniformly recognized that its purpose is "to protect the integrity of the judicial process," by "prohibiting parties from deliberately changing positions according to the exigencies of the moment." Because the rule is intended to prevent "improper use of judicial machinery," judicial estoppel "is an equitable doctrine invoked by a court at its discretion,"
>
> Courts have observed that "[t]he circumstances under which judicial estoppel may appropriately be invoked are probably **not reducible to any general formulation** of principle." Nevertheless, several factors typically inform the decision whether to apply the doctrine in a particular case: First, a party's later position must be "clearly inconsistent" with its earlier position. Second, courts regularly inquire whether the party has succeeded in persuading a court to accept that party's earlier position, so that judicial acceptance of an inconsistent position in a later proceeding would create "the perception that either the first or the second court was misled." Absent success in a prior proceeding, a party's later inconsistent position introduces no "risk of inconsistent court determinations," and thus poses little threat to judicial integrity. A third consideration is whether the party seeking to assert an inconsistent position would derive an unfair advantage or impose an unfair detriment on the opposing party if not estopped.
>
> In enumerating these factors, **we do not establish inflexible prerequisites or an exhaustive formula for determining the applicability of judicial estoppel**.

> Additional considerations may inform the doctrine's application in specific factual contexts.

New Hampshire v. Maine, 532 U.S. 742, 749-51 (2001) (concluding that "judicial estoppel barr[ed] New Hampshire" from taking an inconsistent position and that "considerations of equity persuade . . . that application of judicial estoppel is appropriate in this case") (internal citations omitted) (emphasis added). Relying on New Hampshire v. Maine, the Sixth Circuit discussed the circumstances under which it is appropriate to employ judicial estoppel to prevent a party from changing positions and distinguished arguments made in court from sworn admissions:

> Judicial estoppel seeks to preserve judicial integrity, and the Court has explained that "[a]bsent success in a prior proceeding, a party's later inconsistent position introduces no risk of inconsistent court determinations, and thus poses little threat to judicial integrity." This court has similarly stated that
>
> > before the doctrine of judicial estoppel may be invoked, the prior argument *must* have been accepted by the court. Although this limit allows parties to contradict themselves in court, it threatens only the integrity of the parties, not of the court.
>
> *Teledyne Indus., Inc. v. NLRB,* 911 F.2d 1214, 1218 (6th Cir.1990) (emphasis added).
>
> Aside from the Carrolls' inability to show that United took a "contrary position under oath in a prior proceeding," *id.,* United's offer of judgment contains "no admissions or findings of law or fact." *Id.* at 1219.

Carroll v. United Compucred Collections, Inc., 399 F.3d 620, 624 (6th Cir. 2005). See also United States v. Owens, 54 F.3d 271, 275 (6th Cir. 1995) ("[J]udicial estoppel may apply in contexts when other forms of estoppel do not. . . . Judicial estoppel will be invoked against the government when it conducts what 'appears to be a knowing assault upon the integrity of the judicial system.'") (finding Postal Service judicially estopped); Tyler v. Federal Express Corp., No. 05-6826, 2006 WL 3334953 (6th Cir. 2006) (holding that doctrine of judicial estoppel barred employee's claim against employer where, after she filed her lawsuit, she intentionally, with a motive to conceal the asset, omitted the lawsuit from her Chapter 13 proceedings); State v.

Banks, 271 S.W.3d 90, 146 (Tenn. 2008); In re Merritt Logan, Inc., 109 B.R. 140, 147 (E.D. Pa. 1990) ("As it concerns the integrity of the judicial process, there need be no showing of reliance, privity or prejudice before such estoppel is applied.").

Here, the existence of the second search warrant is an effective admission that the government was required to get a warrant to conduct the forensic examination of the laptop computer. The government's current position with respect to the first warrant is directly inconsistent with the position it took by applying for the second warrant. The government was successful when it took the earlier position, because a search warrant issued. A government agent's sworn statements to a U.S. Magistrate Judge is a categorically different situation than had the government simply continued to deny in its pleadings that it was required to seek a particularized warrant to search the contents of the computer. The Affidavit sworn to by the government agent sought authority to search the computer but did not describe the searching that had occurred to date and admitted (but disavowed) that it is possible to perform a narrowly-tailored search of a computer. Therefore, this is a situation that invokes judicial estoppel because the judicial integrity of the proceedings is at issue.

B. The government disregarded the time limitations set out in both warrants.

At an evidentiary hearing, Mr. Kernell would seek to show that the government disregarded the time limitations set out in both warrants when it searched the laptop computer. Rule 41 of the Federal Rules of Criminal Procedure provides that a warrant "must command the officer to execute the warrant within a specified time no longer than 10 days." Fed. R. Crim. P. 41(e)(2)(A)(i). Both warrants complied with this rule and thereby limited the authority granted to executing officers:

You are hereby commanded to search on or before September 29, 2008.

(09/20/08 *Search Warrant*).

You are hereby commanded to search on or before March 7, 2009.

(02/26/09 *Search Warrant*). The Return for the warrant to search Mr. Kernell's apartment indicates that it was timely executed on September 20, 2008. When the attachments to the second search warrant and its Return were provided to Mr. Kernell today, Mr. Kernell learned that the Return was not filled out or signed.

When a warrant is not executed within the specified time period, evidence found pursuant to its execution should be suppressed. See Sgro v. United States, 287 U.S. 206, 210-11 (1932) (suppressing evidence where warrant not executed within ten days) ("The proceeding by search warrant is a drastic one. Its abuse led to the adoption of the Fourth Amendment, and this, together with legislation regulating the process, should be liberally construed in favor of the individual."). Rule 41 does not contain an exception for computers.

In United States v. Mitchell, 565 F.3d 1347 (11th Cir. 2009), decided April 22, 2009, the Eleventh Circuit held that although the initial warrantless removal of a hard drive from a computer in the defendant's home was permissible, a twenty-one day delay in obtaining a search warrant for the seized computer hard drive was unreasonable under all the circumstances. In Mitchell, the facts showed that the defendant was identified during a federal investigation as having potentially visited a website that contained thousands of images of child pornography, because his credit card showed that he made payments to a bill payment service used by the child pornography website. Id. at 1349. After identifying the defendant, the federal agents went to Mitchell's residence. Mitchell consented to speak with the agents, and even responded "yes, probably" when an agent asked whether either of the two computers (a laptop and a desktop) in

his home contained contraband and child pornography. Id. Mitchell consented to a search of his laptop and signed a consent form. Id.

> After Agent West performed a brief forensic examination of the laptop, he asked Mitchell if he could see the desktop computer. Mitchell assented, and brought the agents to the downstairs office where the computer was located. Upon viewing the desktop computer, Agent West asked Mitchell if that was the computer that contained the child pornography, and Mitchell stated that it was. Agent West then opened the computer's central processing unit ("CPU"), the casing which contains all the internal parts of the computer, and removed the computer's hard drive from the CPU. The agents departed from Mitchell's residence at approximately 12:00 p.m. with only the hard drive.

Id. The next Sunday, Agent West "traveled to Virginia to attend a two-week ICE training course." Id. at 1349. Three days after he returned, he presented an application for a search warrant to a U.S. magistrate judge, who issued it that day, twenty-one days after the hard drive was seized. Id. (noting that "the affidavit in support of the search warrant was twenty-three pages long, but . . . less than three double-spaced pages-was composed of original content"). Acting pursuant to the warrant, Agent West accessed the materials stored on the hard drive and found child pornography images. Id.

Mitchell pled guilty, but preserved his right to appeal from the denial of his motion to suppress. Id. at 1350. On appeal, he argued (1) "that the Warrant Clause of the Fourth Amendment was violated when the law enforcement officers opened the CPU and removed the hard drive" and "that the entire container should have been seized pending the application for a search warrant," even though he conceded that there was probable cause, and (2) "that the twenty-one-day delay in obtaining a search warrant was unreasonable," even if the seizure of the hard drive was proper. The Court dismissed the first argument as a non-issue. Id. at 1350.

Addressing the second issue, the Court noted that "while the initial seizure of the hard drive was permissible, even 'a seizure lawful at its inception can nevertheless violate the Fourth

Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable searches.'"" Id. at 1351 (quoting United States v. Jacobsen, 466 U.S. 109, 124 (1984)). See also id. ("The reasonableness of the delay is determined 'in light of all the facts and circumstances,' and 'on a case-by-case basis.'") (internal citations omitted)).

> Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives. Thus, the detention of the hard drive for over three weeks before a warrant was sought constitutes a significant interference with Mitchell's possessory interest. Nor was that interference eliminated by admissions Mitchell made that provided probable cause for the seizure. As the United States magistrate judge observed: "A defendant's possessory interest in his computer is diminished but not altogether eliminated by such an admission for two reasons: (1) a home computer's hard drive is likely to contain other, non-contraband information of exceptional value to its owner, and (2) until an agent examines the hard drive's contents, he cannot be certain that it actually contains child pornography, for a defendant who admits that his computer contains such images could be lying, factually mistaken, or wrong as a matter of law (by assuming that some image on the computer is unlawful when in fact it is not)." *United States v. Mitchell,* CR407-126, 2007 WL 2915889, at *7 (S.D. Ga. 2007).
>
> While the possessory interest at stake here was substantial, there was no compelling justification for the delay. . . . Although Agent West testified that he was scheduled to depart for a two-week training program in West Virginia on February 28, 2007, this still left two and one-half days after seizing the hard drive before his scheduled departure. Indeed, the twenty-three-page supporting affidavit was largely composed of boiler plate language, and contained less than three double-spaced pages of original content. . . .
>
> The only reason Agent West gave for the twenty-one-day delay in applying for a search warrant was that he "didn't see any urgency" . . . Subsequently, he explained that any sense of urgency was eliminated by Mitchell's admission that the hard drive contained child pornography. . . .

Id. The government argued that the delay had no practical effect on the defendant's rights because Agent West, the only agent specifically trained to conduct a forensic examination, could not have conducted the review until he returned even if a warrant had been obtained. Id. The

U.S. Magistrate Judge, when denying the motion to suppress, also suggested that even if Agent West had secured a warrant on the same day that the hard drive was seized, the evaluation of the hard drive would not have been finished prior to the departure for the training course, because there were "thousands upon thousands of images and the numerous video files" and it took Agent West two weeks just to complete an evaluation of "some of the images." Id. The Eleventh Circuit, though, found these arguments "unpersuasive" because they were based on the false premise that Agent West's absence could have provided an excuse for the delay in applying for the search warrant or, had a warrant been obtained, searching the hard drive.

> The United States magistrate judge correctly observed that "[t]he purpose of securing a search warrant soon after a suspect is dispossessed of a closed container reasonably believed to contain contraband is to ensure its prompt return should the search reveal no such incriminating evidence, for in that event the government would be obligated to return the container (unless it had some other evidentiary value). In the ordinary case, the sooner the warrant issues, the sooner the property owner's possessory rights can be restored if the search reveals nothing incriminating." *Mitchell,* 2007 WL 2915889, at *7. If anything, this consideration applies with even greater force to the hard drive of a computer, which "is the digital equivalent of its owner's home, capable of holding a universe of private information." *Kansas v. Rupnick,* 280 Kan. 720, 125 P.3d 541, 552 (2005). . . .
>
> T]he present case involved the seizure of a single hard drive. No effort was made to obtain a warrant within a reasonable time because law enforcement officers simply believed that there was no rush. Under these circumstances, the twenty-one-day delay was unreasonable.

Id. at 1351-53. In light of the circumstances in this case, the appellate court concluded that the motion to suppress should have been granted and ordered the judgment of conviction reversed.

Here, the computer was seized in September 2008, but the government did not seek a particularized search warrant until February 2009. In Mitchell, a twenty-one day delay in obtaining a search warrant made the initially proper seizure unreasonable. Here, even if the

initial warrant properly allowed the government to seize the computer, the decision not to obtain another warrant for five months makes the continued possession and searching unreasonable.

C. <u>If this Court finds the Second Search Warrant Invalid, the Searches are Not Saved by the Limited First Search Warrant</u>.

The first search warrant authorized the seizure of the computer and a limited number of electronic files. [Doc. 20 at 1]. Mr. Kernell agrees that the first warrant authorized the seizure of the computer but a second was needed to authorize and limit a forensic evaluation. Even if the first search warrant is interpreted to have authorized the government to perform a limited search of the laptop computer, at most it authorized forensic analysts to search for evidence of violations of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B) as set out in paragraph one of the attachment particularizing the items to be seized. This means that the government exceeded the scope of the warrant by searching all parts of the computer for materials for which it had no probable cause. The second search warrant authorized analysis to look for evidence of violations of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B), 1028(a)(7), 1343, 879, 875(c), and 1519. The government said it intends to rely only on the first search warrant but the forensic reports demonstrate that the government searched for more than was even arguably authorized by the first search warrant. <u>See</u> [Doc. 20 at 6-10] (discussing suppression as proper remedy for search that exceeded scope of authority granted by warrant); <u>see e.g.</u>, <u>United States v. King</u>, 227 F3d 732, 750-52 (6th Cir. 2000) (police exceeded scope of warrant authorizing search of first-floor unit by searching basement and search of basement did not fall within good-faith exception to exclusionary rule). When executing officers exceed the scope of a search warrant, the evidence seized must be suppressed. <u>Id.</u>; <u>United States v. Fuccillo</u>, 808 F.2d 173, 177-78 (1st Cir. 1987) (evidence suppressed because executing officers exceeded scope of already overbroad warrant authorizing seizure of women's clothes by seizing 2 racks of men's clothes and declaring that

"the extent to which, in view of the possibilities, the warrant distinguishes, or provides the executing agents with criteria for distinguishing, the contraband from the rest of an individual's possessions" is a test to determine the reasonableness of a general warrant).

The documents that the Court found probable cause to seize pursuant to the September 2008 search warrant were contained in the first paragraph of Attachment B.

> Documents and computer files any in form including but not limited to e-mail, documentation or papers, and digital data that may related or be associated with the screen nicknames rubico and rubico10, the e-mail accounts rubico@yahoo.com and rubico10@yahoo.com, dkrocket@mindspring.com, gov.palin@yahoo.com; Governor Sarah Palin; Facebook; other internet accounts or online services or groups, or hacking activities.

(09/20/08 *Attachment B to Search Warrant* ¶ 1). As pointed out in the original motion, the breadth of a request to seize, for example, "[d]ocuments and computer files in any form . . . related to or associated with . . . other internet accounts or online services or groups, or hacking activities," when combined with the affidavit's request to search "all the stored data" on the computer is too broad to have meaningfully limited executing officers' discretion. See [Doc. 20 at 3, 4]. In addition, several of the "items" are not modified by reference to the crime being investigated. See United States v. Ford, 184 F.3d 566 (6th Cir. 1999) (portions of warrant identified as arguably overbroad where some clauses not limited by reference to illegal activity).

The second search warrant contained a more particularized list of "items to be seized." See (02/26/09 *Attachment B to Search Warrant*). In addition, the second search warrant requested authority to seize items not described in the first search warrant, unless the first warrant is interpreted extremely broadly. See id. ¶ *l* (requesting agents to search for "evidence of user attribution showing who used or owned the Acer computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history").

A warrant must be issued by an impartial judicial officer. See Johnson v. United States, 333 U.S. 10, 13-14 (1948) ("neutral and detached magistrate"); Steagald v. United States, 452 U.S. 204 (1981) (holding warrant necessary because law enforcers "may lack sufficient objectivity to weigh correctly the strength of the evidence supporting the contemplated action against the individual's interests in protecting his own liberty"). The magistrate must consider the facts and circumstances presented in the warrant application and affidavit and make an independent assessment as to whether there is probable cause to conduct a search or to seize evidence. See Aguilar v. Texas, 378 U.S. 108 (1964); Giordenello v. United States, 357 U.S. 480 (1958). The probable cause determination is made at the time the warrant is sought and is not subject to rehabilitation or supplementation by later-acquired or then-uncommunicated information. See Whiteley v. Warden, 401 U.S. 560, 565 n.8 (1971) ("[A]n otherwise insufficient affidavit cannot be rehabilitated by testimony concerning information possessed by the affiant when he sought the warrant but not disclosed to the issuing magistrate. A contrary rule would, of course, render the warrant requirements of the Fourth Amendment meaningless.").

Therefore, the first search warrant cannot provide authority for all of the extensive searching that has taken place, because when the first search warrant issued, it issued based only on the information contained in the first affidavit that was communicated to the neutral magistrate. The nature of the probable cause to search the computer was fixed when the affiant made application for the warrant. Information learned after the first search warrant issued cannot be used to retroactively expand the scope and means of the computer examination. A law enforcement agent directed to execute a search warrant cannot re-define the search while the search is being conducted, because a neutral magistrate must make the probable cause

determination. Searching for more and different things than that for which a warrant grants authority is contrary to the Fourth Amendment.

D. The Questions Raised by the Undisclosed Affidavit Emphasize the Need for an Evidentiary Hearing.

The questions raised by the undisclosed search warrant, as discussed throughout this Motion, emphasize the need for an evidentiary hearing.

1. Re-Stated Reasons Why Mr. Kernell Has Requested An Evidentiary Hearing

In January 2009, Mr. Kernell filed a motion to suppress and requested an evidentiary hearing. [Doc. 20 at 2]. The government's response neither challenged nor addressed the request for an evidentiary hearing, [Doc. 22] but Mr. Kernell's reply referenced his previous request for an evidentiary hearing to explain why the government's response supported the request. [Doc. 27 at 19].

In the government's original response to Mr. Kernell's motion to suppress, the government acknowledged that, "As the Defendant notes, computer searches generally have a two-stage process: 'the physical search for the computer and the later electronic search to retrieve specific data. The Defendant challenges both stages . . . ." [Doc. 22 at 2] (internal citations omitted).

The Motion to Suppress raised whether the government exceeded the scope of the warrant. See [Doc. 20 at 2] (second basis for motion); id. at 7. This issue has several facets. See e.g., [Doc. 20 at 16] (hypothesizing that because "[c]omputers are seized to further search them," that the warrant "effectively permit[ted] government agents to conduct searches of infinite duration and unlimited scope"); [Doc. 20 at 20] (suggesting that the "warrant was executed like a general exploratory warrant"); [Doc. 20 at 18] (asserting a potential invasion of privacy). The motion to suppress was drafted before Mr. Kernell received the computer forensic reports in

discovery, but whether a defendant is entitled to an evidentiary hearing on the execution of a search warrant is not necessarily tied to the receipt of discovery, because a report is only end product of a search and does not reveal the process undertaken by the agents.

2. An evidentiary hearing is necessary to show that an extensive search had occurred at the time of the affidavit in support of the second search.

Whether the government and its agents exceeded the scope of the first and second warrants is the proper subject of an evidentiary hearing. Mr. Kernell is entitled to know what files were searched, how they were searched, how often they were searched and – especially given the existence of the second warrant – when they were searched.

Mr. Kernell has demonstrated the need for an evidentiary hearing regarding the extent to which the forensic evaluation of the computer exceeded judicial authorization. Mr. Kernell does not have access to the government's forensic logs of how the hard drive was examined, the methods of examination. Mr. Kernell was able to inform the Court that the forensic report discloses and includes reports of examination of the email accounts of the previous owners of the computer, the activity of users who had the computer before David Kernell, using an IP address not mentioned in any affidavit as associated with alleged criminal activity. The issues raised by the existence of an additional affidavit and warrant emphasize the need to establish when the searches occurred and call for Agent Wenger's testimony.

IV. CONCLUSION

For the reasons stated above and in the original motion to suppress, Mr. Kernell respectfully asks this Court to hold an evidentiary hearing and to enter an order suppressing all evidence obtained as a result of the unlawful search of the computer.

Respectfully submitted this 27th day of July, 2009

RITCHIE, DILLARD & DAVIES, P.C.

/s/ WADE V. DAVIES

/s/ANNE E. PASSINO

WADE V. DAVIES [BPR #016052]
ANNE E. PASSINO [BPR #027456]
606 W. Main Street, Suite 300
P. O. Box 1126
Knoxville, TN 37901-1126
(865) 637-0661
Counsel for David C. Kernell

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and exact copy of the foregoing has been filed electronically this 27th day of July, 2009. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. Parties may access this filing through the Court's electronic filing system.

/s/ Wade V. Davies
WADE V. DAVIES